



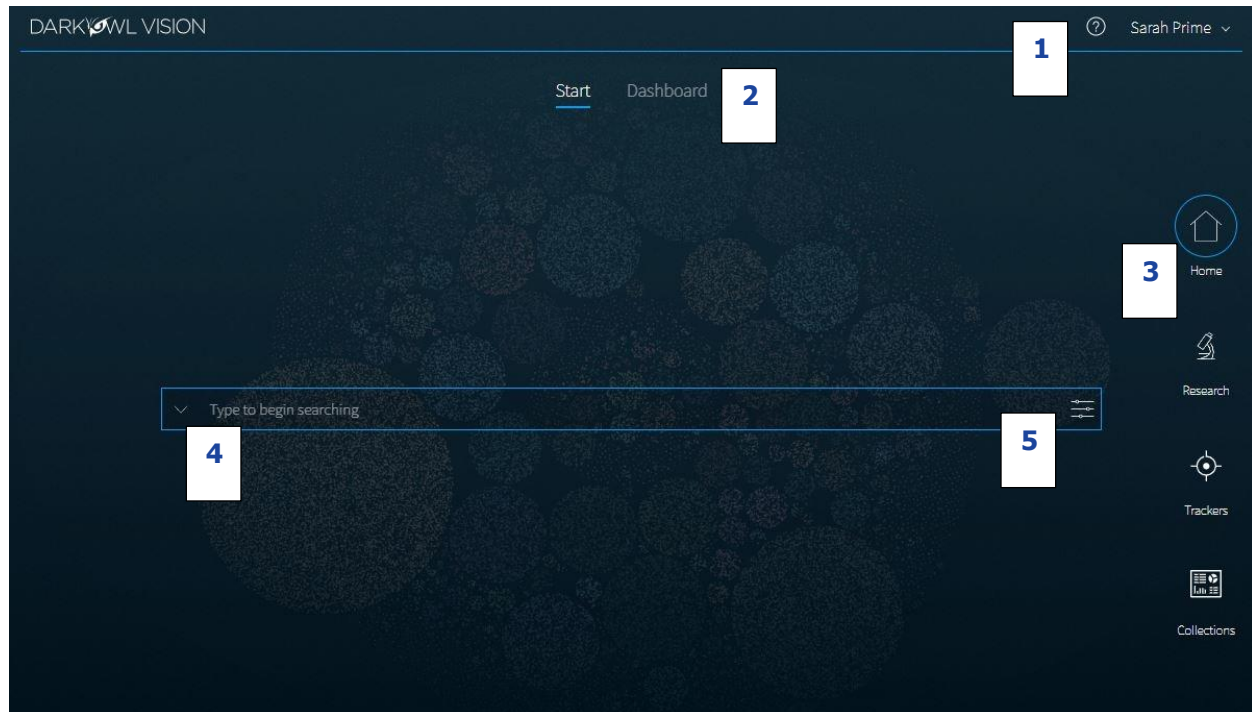
DarkOwl Vision User Interface Guide

Table of Contents




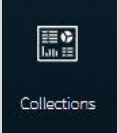
Getting Started	3
Searching	4
Using the Search Bar	4
Search Bar Help.....	5
Search Techniques.....	5
Filters, Dates, and Advanced Search Options	9
Search Tools.....	12
Templates	12
Entity Search.....	12
Lexicon	13
Query Builders.....	14
Search Blocks	15
Data Networks and Search Results.....	17
Search Result Viewer	17
Viewing Individual Result Detail	18
Saving Searches	19
Your Collections: Saved Searches Page	20
Editing a Saved Search	20
Your Trackers: Alerts Page	21
Alerts Page and Viewing Alerts	21
Deleting Alerts.....	21
Your Trackers: DARKINT Exposure.....	22
Setting Up a Score.....	23
The DARKINT Score Formula.....	24
Viewing Scores Over Time.....	24

Getting Started

DarkOwl Vision's user-friendly User Interface has tools that enable analysts to effectively search, monitor, and receive alerts when leaked data appears on the darknet.



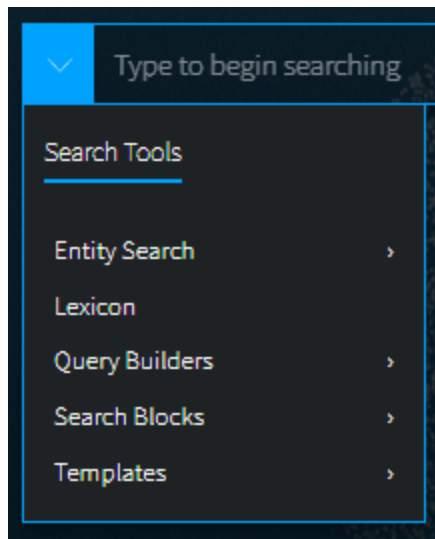
- | | |
|---|--|
| 1. Help & Account Options | A quick link to Help resources; clicking on your name opens a menu to change your password or logout. |
| 2. Start / Dashboard Toggle | Toggle between simple search view, or Dashboard at-a-glance view of Alerts, DARKINT Exposure, Recent Searches, and Saved Searches. |
| 3. Right Navigation Menu (see below) | Navigate to Research to view search results; Trackers (Alerts & DARKINT Exposure); your Collections of Searches and Blocks. |
| 4. Search Bar | Type to begin searching or click on the arrow to open the Search Tools menu to find tools to help you create your search. |
| 5. Filters Menu | Create a targeted and effective search using filters, dates, and advanced options. |

			
Start / Dashboard pages	Search Results page	Alerts / Exposure pages	Saved Searches / Search Blocks pages

Searching

Using the Search Bar

1. The search bar works like most search engines; simply type words, phrases, numbers, or characters. The [Search Techniques](#) section goes into more detail and options for searching, but here a few quick start tips:
 - Use Boolean operators when searching more than one keyword. See: [Searching with Booleans](#).
 - Use quotations ("**Jane Doe**") to send the query as one phrase, *Jane Doe*.
 - Use the **exact:** search operator (**exact:fullz**) to prevent word stemming, and search for exact matches of that term. See: [Stemming and Searching for Exact Terms](#).
2. Use the left drop-down menu to open **Search Tools**, which include:



Entity Search: the best way to search for Emails, Credit Cards, Cryptocurrency Addresses, IP Addresses, and Social Security Numbers in our system. You can also create Search Blocks from these builders.

Lexicon: curated lists of commonly searched items and different areas of content in our database.

Query Builder: a helper for search variations or advanced formatting for commonly search items.

Search Blocks: Pre-populated keyword as well as any custom search blocks that you create, are accessible from this menu for easy access.

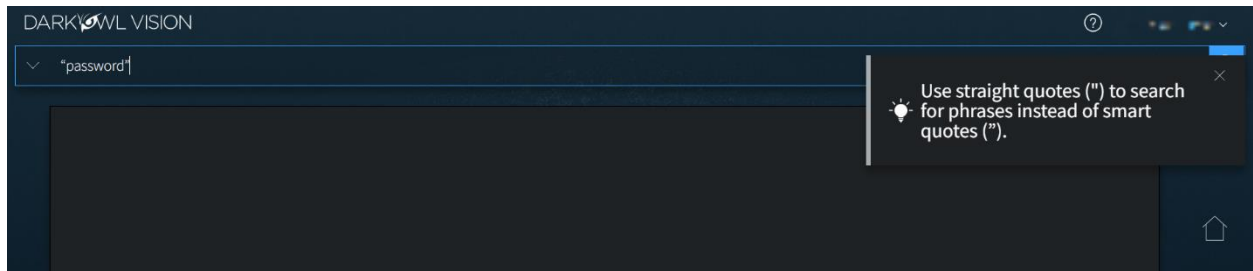
Templates: pre-populated search templates to help you get started quickly.

Once you've started searching, **Recent Searches** and **Saved Searches** will also appear in this menu, for easy access.

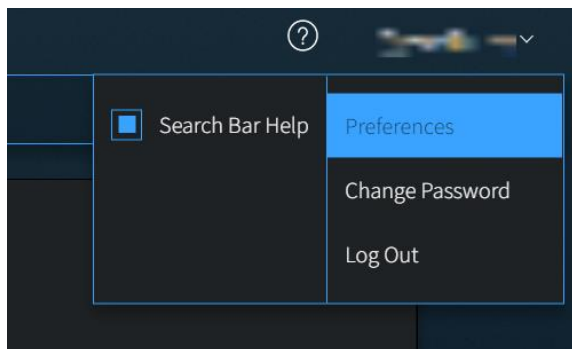
3. Click on the right Filter menu to refine your search, create targeted queries, and select options. More information about these is provided in this section: [Filters, Dates, Advanced Search Options](#).

Search Bar Help

Search tips will appear in the upper right corner when a search could be optimized or includes a character the field doesn't recognize.



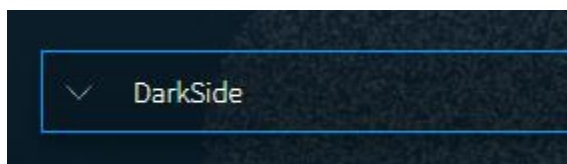
You can turn this feature off by clicking on your name in the upper right corner, selecting Preferences in the drop-down menu, and unchecking the toggle for Search Bar Help.



Search Techniques

Single Terms

To find any document containing a specific keyword, simply put that keyword into the search bar:



Phrase Searching

To find two or more keywords in a specific order, place the keywords within double quotes:

- **"AES 256"**

Without the double quotes, the search would be sent as: *AES OR 256*. This search is an inclusive search and may return results that only include the term AES, that only include the term 256, that include both terms but not next to each other, and that include both terms next to each other.

Boolean Searching

Use Boolean operators **AND**, **OR**, and **NOT** to specify inclusions, alternate terms, or exclusions. (You can substitute AND, OR, and NOT with **&&**, **|**, and **!** respectively.) Keywords and field searches can be separated by any of the above in order to fine-tune your results.

- **drugs OR crime** – find documents with either 'drugs' or 'crime'
- **drugs AND crime** – find documents with both 'drugs' and 'crime'
- **DarkOwl AND (hack OR ddos OR 0day)** – find documents with DarkOwl and any one of three hacking keywords

Note: Boolean operators must be in all caps. If they aren't in all caps, DarkOwl Vision will consider the word "and", "or", etc as keywords.

Using Subqueries/Boolean Order of Operations

You can group together phrases to form subqueries, using parentheses () to indicate each clause. This is especially important when both ANDs and ORs are used, to designate the correct order of operations for your subqueries.

- **DarkOwl AND (drugs OR crime)** – find documents with DarkOwl and either drugs or crime
- **("AES-256" OR "AES 256") AND ("RSA-4096" OR "RSA 4096")** – find documents with one of AES-256 or AES 256 and one of RSA-4096 or RSA 4096

Stemming and Searching for Exact Terms

DarkOwl Vision supports a process called *stemming*, which tries to reduce a word to an approximation of its stem or root form. Usually, terms are stemmed to plural/singular versions or different tenses. This means that searching will return matches on related forms of a word, unless you specify otherwise:

- **Hack** may return **Hacked, Hacker, Hacking**, in addition to **Hack**

When you want to search for a specific term, including special characters and punctuation, use the **exact:** operator to prevent word stemming:

- **exact:hack** – will return only documents containing the word hack

Excluding Items from a Search

Keywords can be excluded in multiple ways:

- Using the 'NOT' Boolean operator
- Prefacing the term with a hyphen
- Prefacing the term with an exclamation mark

For example, the three searches below are equivalent and will find documents that contain 'DarkOwl' but not 'drugs'. Note that when excluding a keyword via hyphen or exclamation mark, it must be placed directly before the keyword with no space in between.

- DarkOwl NOT drugs
- DarkOwl -drugs

- DarkOwl !drugs

You can also exclude values in other fields in the same way:

- DarkOwl NOT domain:drugs.onion
- DarkOwl -domain:drugs.onion
- DarkOwl !domain:drugs.onion

Searching for Entities in the Search Bar

When searching for specific entities, such as an email address or credit card number, directly in the search bar, always use the designated search operator. The Search Tools (in the drop-down on the left-side of the search bar) are a shortcut and automatically convert your query to the correct syntax.

- email:first.last@company.com
- ccn:111111111111111111
- cryptocurrency:15ivMrk8VzaK9TEN85XYssVbU3Yd6tLzb9
- ipAddress:127.0.0.1\24
- ssn:123-45-6789

When searching for multiple entities, use the search operator and a Boolean OR, as follows:

- email:(first.last@company.com OR last.first@company.com)
- ccn:(111111111111111111 OR 222222222222222222)

Searching for both Keywords and Entities in the Search Bar

When searching for both keywords and specific entities (such as an email address or credit card number) directly in the search bar, use the following format:

- ("First Last" OR Nickname) AND email:first.last@company.com

Using Wildcards

Wildcards (* or ?) are currently allowed *in limited usage*, in the middle or end of terms only. (*) is used to find *zero or more* unknown characters; (?) is used to find *any one* unknown character. Examples:

- **dar*** – will find "dar", "dart", "darkowl", "daredevil", etc
- **d?rk** – will find "dark", "dork", "dirk", etc; will not find "drk" (however, **d*rk** would)

DarkOwl Vision does not support *leading wildcards*. In other words, a search term cannot begin with either one of the wildcard characters.

Using Proximity Searches

You can find words in proximity to each other by using quotations and selecting a maximum distance allowed: "**password hack**"~2. We support a maximum distance of 9.

Using Pattern Matching / Regular Expressions

Lucene-based regular expressions are allowed and should be wrapped by forward slashes (/). Not all functionality you may be familiar with may be supported. Additionally:

- **These queries may time out**, particularly when searching for a high volume of unknown characters. Regex searching is computationally heavy and will result in slower, less performant searches.

To use a regular expression in Vision, place the expression between two forward slash characters:

- **/r[0-9a-zA-Z]{24,34}/** – to find results matching the pattern of a Ripple cryptocurrency address (which starts with 'r', then has anywhere between 24 to 34 alphanumeric characters)

Note: Not all regex functionality you may be used to is supported by our system.

Using Special Characters

The following characters are reserved:

+ - = && | | > < ! () { } [] ^ " ~ * ? : \ /

If any of the above characters are in a keyword or phrase being searched, you can escape the character with a backslash: \. For example, to search for mentions of a URL within a document, such as *https://darkowl.com/darkint-blog*, you must escape the colon, forward slashes, and hyphen, otherwise the search will return an error.

You can perform this search multiple ways:

1. Escaping the special characters: **https\\:\\\\darkowl.com\\darkint-blog**
2. Putting the whole keyword in quotes: **"https://darkowl.com/darkint-blog"**

Without escaping the special characters, this search will be interpreted as:

- Searching within a field called 'https' (which doesn't exist) for:
 - An empty regular expression (// signifies the start and end of a regex with no content)
 - The keyword 'darkowl.com'
 - The start of a regular expression starting with 'darkint-blog'
 - No end to the regular expression (will return an error)

Field Searching (Search Operators for Metadata Searches)

Every search performed will look in one or more fields for the keyword(s) being searched. By default, the search bar will search both the 'title' and 'body' fields of documents. This means that results will be returned if the keywords you're looking for are found in either the body of the document or the title (or both). For example, a search of just **the word 'drugs' in the search bar** is equivalent to:

title:drugs OR body:drugs.

Most searches will not require specifying a field name, since title and body are automatically searched. However, other metadata fields can be searched in addition to title and body, for example:

- **title:alphabay**
- **hackishness:1**
- **domain:drugs.onion**

The list of metadata fields is below. When searching within these fields, type the following search operators in the search bar, and then the query content:

- inUrl:
- contentType:
- headers.server:
- headers.last-modified:
- title: (to search within this field exclusively)
- body: (to search within this field exclusively)
- domain:
- leak:
- network:
- hackishness:

Multiple values within the same field can be searched in a number of ways. The following examples are equivalent:

- **domain:(drugs.onion OR crime.onion)**
- **domain:drugs.onion OR domain:crime.onion**

You can also look for phrases within specific fields using double quotes:

- **title:"Forum rules"**

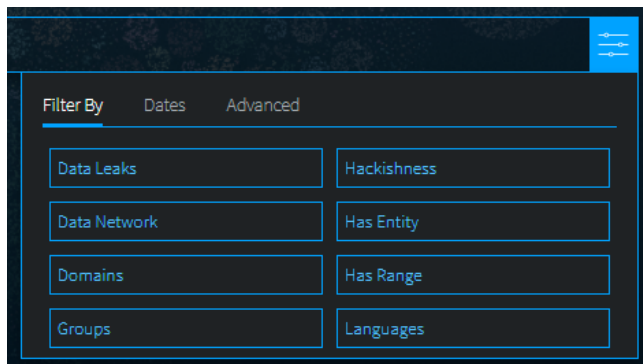
Subqueries within fields are supported:

- **title:(darkowl AND (drugs OR crime))**

Note: when searching using fields, there should not be a space after the ':' character.

Filters, Dates, and Advanced Search Options

Refine your search with filter and date options using the Filters icon on the right side of the search bar.



Data Leaks

Filter to content from known breaches or other leak data, tagged by name in DarkOwl Vision. See the Lexicon for descriptions of the Data Leaks in this list. Type or scroll to find the desired Data Leak. **Click once to include, click twice to exclude.**

- For free text searching, type *leak:leakname* in the search bar, prefixing with - to exclude.

Data Network

Filter to content from a particular DarkOwl data collection network. Options include: Discord, FTP, I2P, IRC, Onion, OpenNIC, Telegram, Zeronet. **Click once to include, click twice to exclude.** More information: [Data Networks](#).

- For free text searching, type *network:networkname* in the search bar, prefixing with - to exclude.

Domains

Filter to content from one or more domains, or exclude a particular domain by typing a hyphen in front of the domain. Type only the domain portion (such as, **arch3rsecgjqcmjb.onion**; no need for the www or http:// prefix) in the filter box. Be sure to remove any trailing slashes or paths from the domain.

- For free text searching, type *domain:domain.com* in the search bar, prefixing with - to exclude.

Groups

Groups are combined filters that narrow your search to specific categories; **click to include:**

- *Authenticated Sites*: Filter to content from sites requiring credentials or other challenges.
- *Blogs*: Filter to content from sites identified as blogs.
- *Chans*: Filter to content from a curated set of chan/imageboard forums selected by our analysts.
- *Darknet*: Filter to content from the Tor, I2P, and Zeronet darknets.
- *Forums*: Filter to content from sites identified as forums.
- *Markets*: Filter to content from sites identified as darknet marketplaces or vendor shops.
- *Ransomware*: Filter to content from known ransomware sites.
- *Paste Sites*: Filter to content from a curated set of paste sites selected by our analysts.

Hackishness

Hackishness assigns a rating to every piece of content collected, indicating the likelihood to which the information could be used for criminal activity. The lower bound of hackishness is .01 and the upper bound is 1.0; the UI shows these as percentages on search results. You can quickly filter to results with hackishness by **using the slider** on the Hackishness filter to select a desired hackishness threshold.

You can also filter to hackish results using hackishness: in the search bar, which supports searching as range. This means, you can narrow down to values between two parameters, *inclusive or exclusive*, for example:

- **hackishness:[.01 TO 1]**
- **hackishness:{.01 TO 1}**

Note the '[' and '{' characters used above. In Lucene range queries, '[' and ']' are inclusive so the first query above would return values from .01 to 1, including both .01 and 1. The second example would return values from .01 to 1 not including .01 or 1. '[' and '{' can be combined:

- **hackishness:{.5 TO 1]**

The above will find values greater than .5 and up to and including 1.

[Has Entity \(Credit Cards, Cryptocurrencies, Email, IPs, Social Security Numbers\)](#)

Filter to content that have at least one selected Entity. **Click next to the Entity name to select.**

[Has Range \(Credit Cards, Cryptocurrencies, Email, IPs, Social Security Numbers\)](#)

Filter to content that have a certain number of selected Entities. This filter is helpful in finding "dumps," as many threat actors will post multiple instances of PII on a singular site or document. **Type values next to a selected Entity.** Enter a lower bound (minimum 1), upper bound (maximum 999999), or use both fields to form a range (50 to 1000).

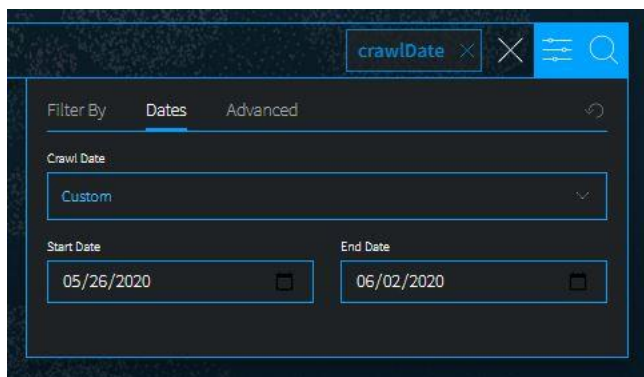
[Language](#)

Filter to content in a particular language. Languages are detected by DarkOwl Vision at the time of ingestion, using natural language processing. **Click once to include.**

- For free text searching, type *language:languagevalue* in the search bar, prefixing with - to exclude.

[Dates](#)

Use the drop-down to quickly select a time range for search results, or select *Custom* to choose a specific start/end date.



Crawl dates can be searched in the search bar as a range using the following date format: YYYY-MM-DDTHH-MM-SSZ:

- **crawlDate:[2021-07-01T00:00:00Z TO 2021-07-10T23:59:59Z]**

As crawlDate supports range searching, you can narrow down to values between two parameters, *inclusive or exclusive*, as discussed in the hackishness section. In Lucene range queries, '[' and ']' are inclusive, and '{' and '}' are exclusive.

Advanced Options (Sort By, Show Similar, Empty Bodies)

Use Advanced Options to select a Sort option, or to show all results (including duplicates).

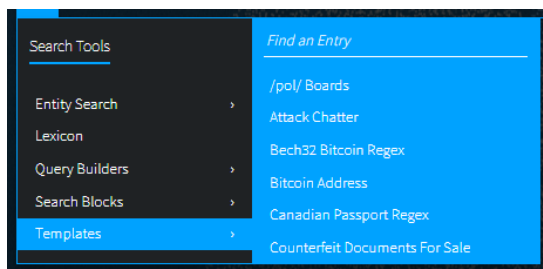
- **Sort options.** Use the drop-down to sort your results by **Relevance** (default), By **Hackishness**, By **Crawl Date**
- **De-duplicate your results.** You can choose to de-duplicate your result sets or see all results, including similar results. The default is to de-duplicate result sets; you can toggle this on or off.
- **Empty bodies.** Our collection includes documents collected that do not contain any text characters; text content is stored in the Body field. Use the drop-down to select Any document (documents can include text in the body, or no text in the body); Results must have body field (to only return documents that had text content on them); or Results must not have body (to see only documents without text).

Search Tools

The Search Tools menu includes tools to help you create effective searches, including **Entity Search**, the DARKINT **Lexicon**, **Query Builders**, **Search Blocks**, and **Templates**. Once active, your **Recent Searches** and **Saved Searches** will also appear in this menu for easy access.

Templates

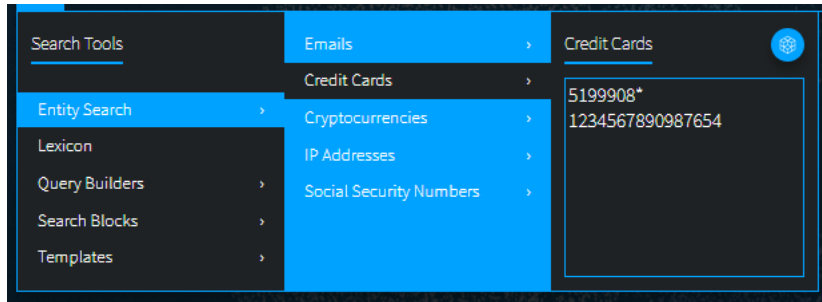
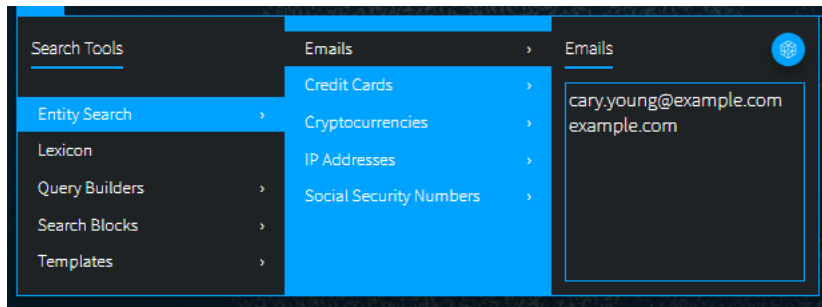
Search **Templates** are a great way to get started searching our data. This list includes many example searches to help find information of interest. Click on a description to populate in the search bar; if indicated, replace the text with your information as appropriate (for example, when "organization.com" appears in the template). Start typing in the *Find an Entry* field to filter the list quickly.



Entity Search

Entity Search is the best way to search within our indexed document collection for Emails, Cryptocurrency, Credit Cards, IP Addresses, and Social Security Numbers. Additionally, all Entity Searches can easily become **Search Blocks**, by clicking on the Search Block icon on the upper right.

- Email supports searching for *individual addresses, domains, or subdomains*.
- Credit Cards supports searching for *individual addresses or BINs*.
- Cryptocurrency supports searching for the following types: *Bitcoin, Ethereum, Monero, Litecoin, Dash, ZCash*. The types have been validated by DarkOwl Vision. Cryptocurrency wallet types not in this list can continue to be found with regular expressions.
- IP Address supports searching for the following formats: *IPv4, IPv6/IPv6 compressed, and CIDR ranges for both IPv4 and IPv6*.



Lexicon

The **DARKINT Search Lexicon** includes curated lists of commonly searched keywords, domains, or data leaks, intended to help you find interesting content within our data collection. While not an exhaustive list of items in our data, it's a good place to get started. The Lexicon continues to grow as we add more content and hear from our customers. If you know of a new threat actor or darknet marketplace that's not in our list – please let us know about it at <https://www.darkowl.com/lexicon>.

To use the Lexicon, pick a topic on the left, then filter or scroll to find entries of interest. Selecting the box next to your desired entry(ies) will immediately add the entry(ies) to the search bar.

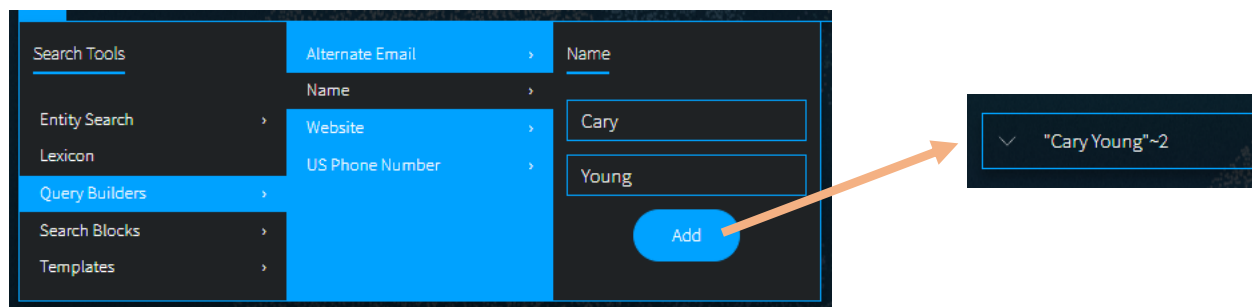
Topics You'll Find in the Lexicon

Actors	<p>Use the Actor lexicon to find actor names mentioned within search results. Actors are malicious individuals or groups that carry out targeted attacks or campaigns, with motives ranging from political hactivism to cybercrime. Many of the actors in the Lexicon come from this list from MITRE.</p> <p>Note: with the Actor and Vendor lexicons, it may be helpful to use additional search terms to reduce false positive results with Actor names that are also common words, such as <i>(HACK CRACK FULLZ EXFILTRATION DDOS)</i>.</p>
Data Leaks	<p>Use the Data Leaks lexicon to find search results from known breaches or other leak data that are tagged by name in our data. A description of each breach is included.</p>
Exploits	<p>Use the Exploits lexicon to find exploit names mentioned within search results. Exploits are software tools designed to capitalize on flaws in a computer system, typically for malicious purposes. Examples: trojans, malware, viruses, RATs, ransomware, botnets.</p>

Forums	Use the Forums lexicon to find search results from known darknet and deep web forms. Forums are online places where people discuss specific topic threads. Some require authentication to access. Forums that are associated with specific markets and/or vendor reviews are indicated.
Markets	Use the Markets lexicon to find search results from known darknet market domains and vendor shops. Content includes both small, vendor-owned markets, to big-name marketplaces such as Hydra and Empire. Some marketplaces have previously been taken down by law enforcement, though our data collection may still have historical content.
Ransomware Services	Use the Ransomware Services lexicon to find search results from domains administered by ransomware gangs. Each entry includes a description of when the gang was first active, associates and affiliates, and encryption cipher used.
Vendors	Use the Vendors lexicon to find vendor names mentioned within search results. Vendors are sellers of goods or services on darknet marketplaces or forums. Each vendor in the Lexicon includes markets or forums where the vendor is active.

Query Builders

Query Builders help you format commonly searched items that either require special formatting or work best when submitted with variations, in order to make the most inclusive search to find the best results. Select the type of builder (descriptions below), input text in the appropriate field(s), and click Add. This will format the query and place it in the search bar. You can continue to add filters, date ranges, or other advanced options before submitting the search.

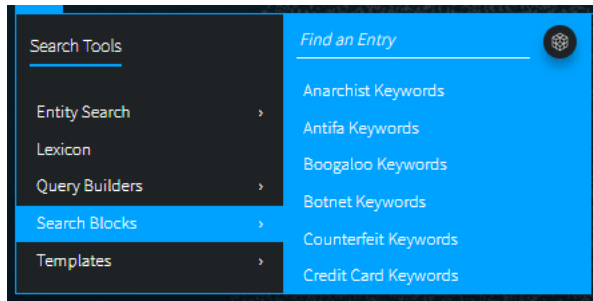


- **Alternate Email:** When searching for email addresses a threat actor may be using with another provider, a trailing wildcard can be a helpful search. For example, entering the prefix of Conti44 in the Query Builder will find results for conti44[at]hotmail.com, conti44[at]hotmail.il, conti44[at]tutonota.com, and so forth. These may be potential associated or alternate email addresses.
- **Names:** When searching for first and last names, we recommend using a proximity search, with up to 2 words as a distance. This can help find variations such as "last, first" or "first middle last" (even when the middle name is unknown).
- **Websites:** When searching for domain/URL mentions within the body of a document, we recommend this format to find variations that start with https://, or www, or any path.

- **US Phone Numbers:** When searching for US phone numbers, we recommend preparing a query without spaces and with spaces between number groups.

Search Blocks

Search Blocks are reusable search components and appear in Search Tools for quick access. Use Search Blocks to create lists of commonly searched items, such as a list of company names, IPs, or domains; or create any query string that you'd like to use across multiple searches.



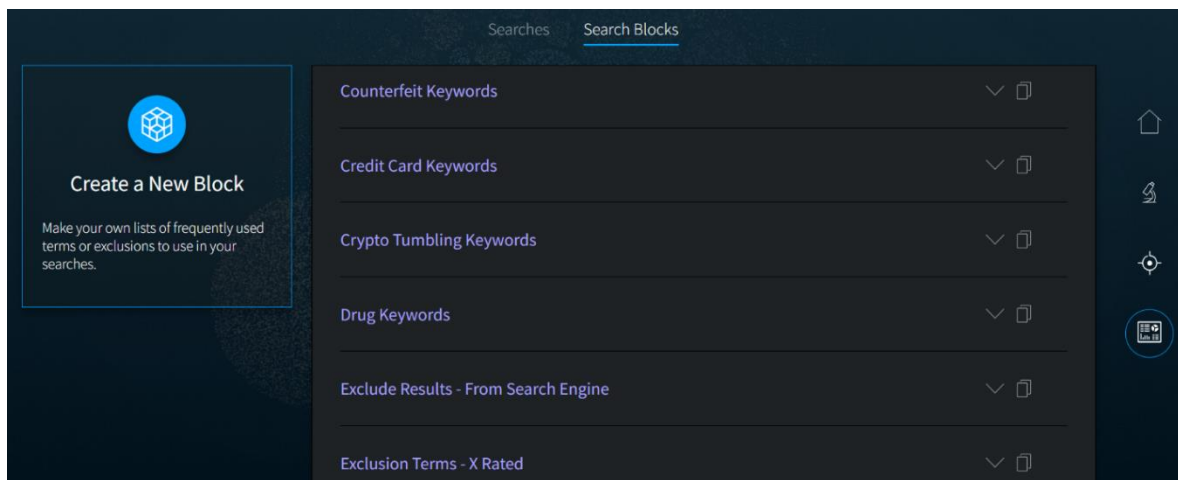
You can use the same block in multiple searches, which can help save you time when you are building queries that have similar elements. Additionally, when you update a block, all searches that use that block are automatically updated to use the new block content.

Initially you'll see a list of pre-built blocks in the Search Tools list and Search Block page, which were created by DarkOwl analysts. After you create your own search blocks, they will appear at the top of the list. Begin typing in the Find an Entry field to filter the list.

You can make search blocks in a few different ways:

- Select **Create a New Block** on the Collections: Search Blocks page build a new list from scratch.
- On the Search Blocks page, click on the Edit icon next to a pre-built block. Make modifications and save as a new block.
- When you are in the Entity Search, click on the block icon to convert into a new block.

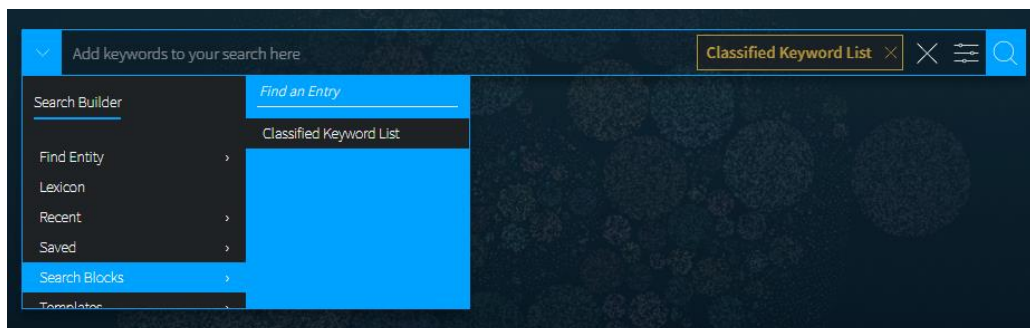
You can manage your Search Blocks on the **Collections: Search Blocks** page. Pre-built blocks include curated keyword lists, as well as blocks that help you exclude terms.



Creating a Search Block

1. Click **Create a New Block**.
2. Open the Select a Block Type drop-down, and choose from: Free Text, Credit Cards, Cryptocurrencies, Domains, Emails, IP Addresses, or Social Security Numbers.
 - **Free Text** accepts the same inputs and formatting (Booleans, operators, etc) as free text on the search bar.
 - **Credit Cards** can be lists of individual credit card numbers or BINs. If entering BINs, use a trailing wildcard after the first six numerical digits.
 - **Cryptocurrencies** can be lists of cryptocurrency wallet addresses. Supported types include *Bitcoin*, *Ethereum*, *Monero*, *Litecoin*, *Dash*, *ZCash*.
 - **Domains** allow you to *filter to content from selected domains*. Use the Free Text Block Type to search for domain mentions.
 - **Emails** can be lists of email addresses, email domains (without the @ portion), or email subdomains.
 - **IPs** can be lists of IP addresses. We support the following types: *IPv4*, *IPv6/IPv6 compressed*, *CIDR ranges for both IPv4 and IPv6*.
 - **Social Security Numbers** should be input using hyphens (i.e. 123-45-6789).
3. Next, input your desired Block Content.
4. Finally, give the Block a Nickname and click Submit.

Once created, your block will now be accessible through the Search Tools > Search Blocks. Click on the block to add it to your query on the search bar.



Viewing the Content of a Search Block

On your **Collections: Search Blocks** page, use the arrow to show/hide your search block content.

Copying a Pre-built Search Block

On your **Collections: Search Blocks** page, click the Copy icon next to the desired block. Make your revisions directly in the Block Content field, update the Block Nickname, and click Submit. This block will now appear as a new block.

Editing a Search Block

On your **Collections: Search Blocks** page, click the Edit icon next to the desired block. Make your revisions and click Submit. If this block is used in automated searches, the next time the search runs, it will use the new block content you've specified.

Deleting a Search Block

On your **Collections: Search Blocks** page, click the Delete icon next to the desired block. If this block is not used in any current searches, click *Delete* to confirm. If this block is used in saved searches, you will be prompted to go to the Saved Searches page to edit these searches to remove the block(s). Otherwise, click *Delete Block and Searches* to confirm.

Data Networks and Search Results

DarkOwl Vision data collection is automated and continuous 24/7/365, collecting content from millions of websites daily in 47 languages. Currently, our collection includes Tor, I2P, Zeronet darknets; encrypted chat servers, channels, and groups; certain deep web sites with transitory information, such as paste sites, forums, and FTP content; as well as high-interest closed access surface web sites. Collectively, we refer to this as **DARKINT™**, or **darknet intelligence**.

The information that we collect from these networks is parsed into the following field categories:

Body field	The raw text collected from the webpage/record/target.
Metadata fields	Fields we collect along with the body, if available, such as: domain, network, language, headers. Click on the Metadata and Leak view switches in Search Results to see this information.
Mined fields	Tokenized entities we mine out of the body of the result, which are currently: <i>emails, credit cards, cryptocurrencies, ip addresses, and ssns</i> . These appear as individual View Switches in Search Results, if present in the body. <i>When searching for entities, either use the Search Tools menu > Entity Search or prefix with the appropriate search operators in the Search Bar.</i>
Processed fields	Information we apply to a result from our natural language processing or machine learning, such as <i>hackishness</i> or <i>language</i> detection.

Search Result Viewer

After running a search, your result list will appear on the Research page. The list displays a summary including an excerpt from the result (around the first keyword match, if applicable), keyword hits (if applicable), where the result was found, crawl date, hackishness, and relevance of the result.

Click on an Excerpt to open the full Result Detail; click again to close the Result Detail.

Keyboard Shortcuts

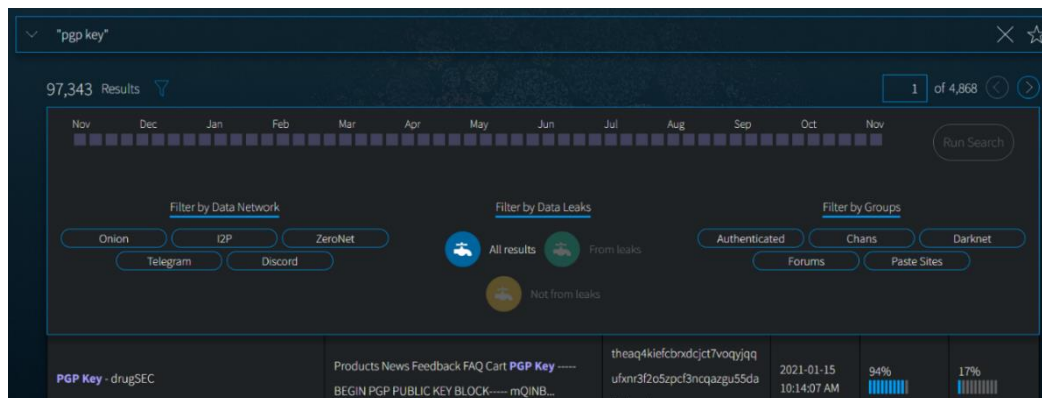
Navigate through Search Results using these keyboard shortcuts:

Key	Description
k	next result
i	previous result
l	next highlight

j	previous highlight
;	toggle detail pane
o	next page
u	previous page

Quick Filtering

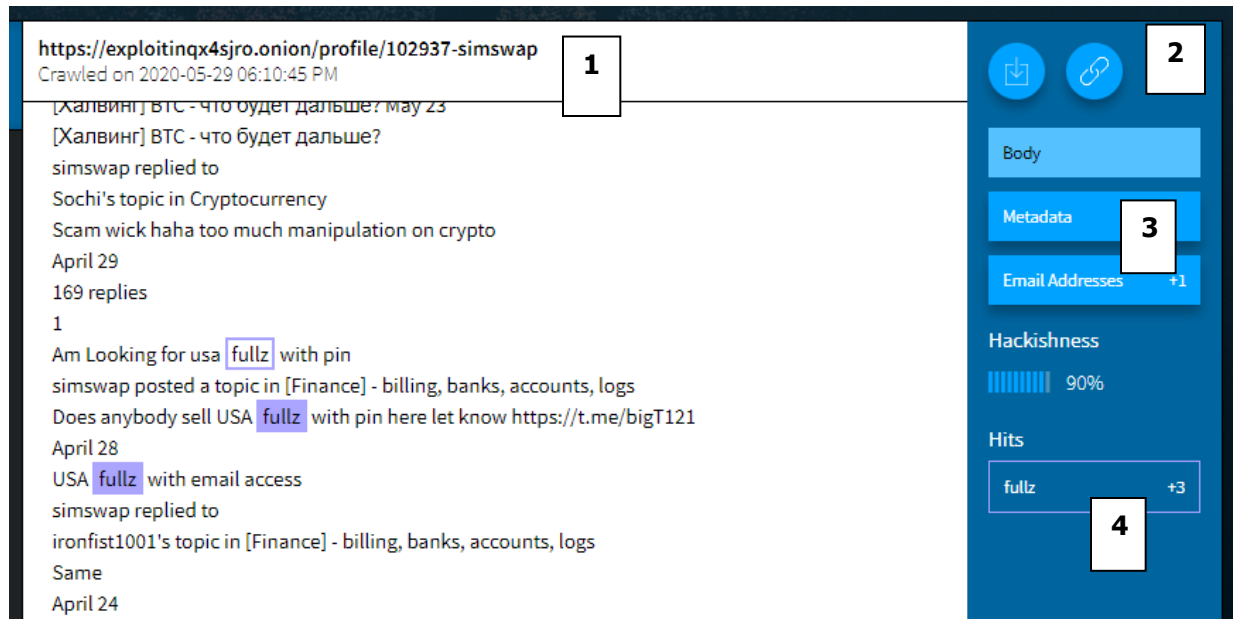
The icon next to the number of search results will open a Quick Filter menu. This menu includes some of our most frequently used filters and can help refine your result set. Once selected, filters will appear in the search bar. Click the **Run Search** button to see a new result list.



- **Crawl Date Slider.** Select a Crawl Date range within the last year, by clicking on a box to start, sliding over the date period, and clicking on an end box.
- **Filter by Data Network.** Click once to select a network; click twice to exclude a network.
- **Filter by Data Leak.**
 - Select *From leaks* to see only results from Data Leaks
 - Select *Not from leaks* to exclude results from Data Leaks
- **Filter by Groups.** Click once to select a group; click twice to exclude a group.

Viewing Individual Result Detail

1. **Source** of the result and when we added it to our data collection.
2. Options to **Download** the result or get a **Link** to return to this result later.
3. View switch buttons to see **Metadata** about the result, **Lists of Entities** found in the result (emails, cryptocurrencies, cards, ip addresses, SSNs, if available), or return to the **Body**, or content of the result. An additional view switch button, **Leak Info**, will be present if the result is from a data leak.
4. Use the **J and L keys on your keyboard** to surf through the **Hits** that match your query terms.

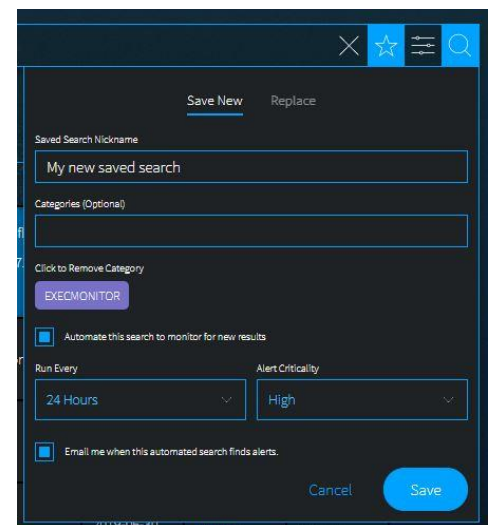


Saving Searches

A **Saved Search** is simply a query you'd like to run again in the future. Choose to **Automate this search** to apply monitoring functionality, which generates **Alerts** on your dashboard if hits are found.

After you run a query, the Save Search icon (star icon) will appear on the right side of the search bar. Selecting that icon will open a form; fill in the appropriate fields:

- Add a **Saved Search Nickname**.
- Add **Categories**, if desired. Categories can help you sort your searches and alerts.
- Click **Automate this search**, if you'd like to apply monitoring. If this is selected, additional options for *Frequency*, *Criticality*, and *Email Notifications* will appear.
- Click **Save** when complete.



Your Collections: Saved Searches Page

Access your **Saved Searches** page from the Collections right navigation icon. Click on a Name to open the Search Detail. Here, you can:

1. Change the name or categories associated with the search
2. Enable/disable automated searching
3. Adjust the run frequency or desired criticality of Alerts from the search
4. Run the search, or make edits to the search (more information: [Editing a Saved Search](#))
5. View Alerts from the search (if any)

The screenshot displays the 'Saved Searches' interface. On the left, a list of searches includes 'Bitcoin Regex', 'CCNs on Telegram' (selected), 'Cisco Emails', 'CVE Exploit Mentions', and 'IRC Channel Mentions'. The central area shows the configuration for 'CCNs on Telegram'. It includes a 'Name' field, a 'Categories' field, a 'Click to Remove Category' button, a 'CARDING' button, an 'Automate search' checkbox, an 'Email me when this search finds alerts' checkbox, an 'Interval' dropdown menu (set to 6 Hours), and a 'Criticality' dropdown menu (set to Low). The right sidebar contains buttons for 'Run Search', 'Edit Search', and 'Alerts', along with 'Last Run' and 'Next Run' timestamps. Numbered callouts 1 through 5 highlight specific features: 1 points to the search name field, 2 points to the 'Automate search' checkbox, 3 points to the 'Interval' dropdown menu, 4 points to the 'Run Search' button, and 5 points to the 'Alerts' section.

Editing a Saved Search

From the Searches page in your Collections, choose the search you'd like to adjust, then click Edit Search. This will bring you to the Research page, with your current search pre-populated in the search bar. From here, you can make changes to your search, updating filters, adding keywords, etc. Once you have made adjustments, run the search.

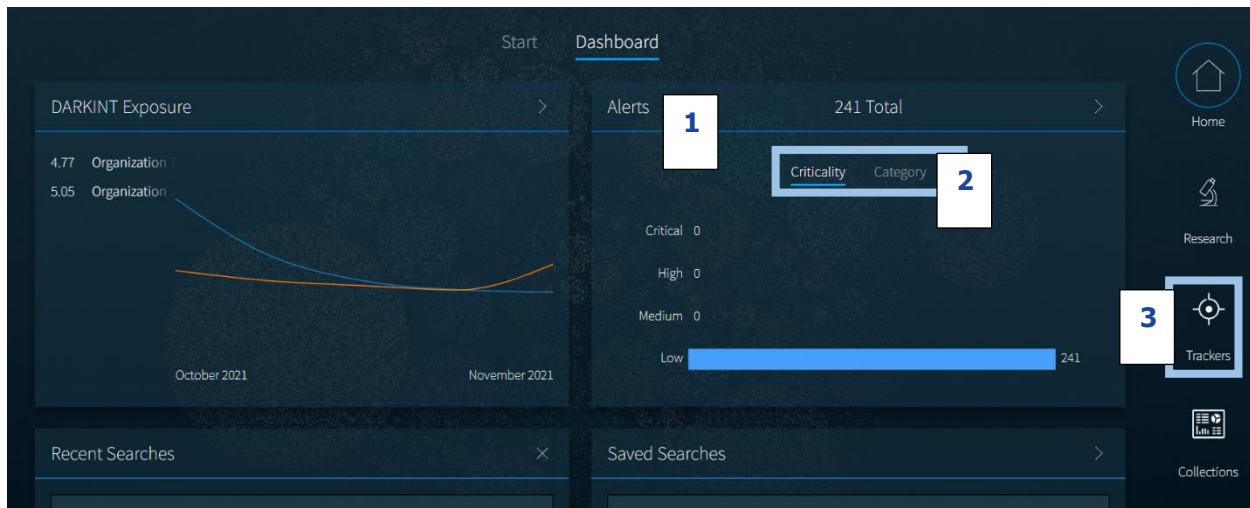
The Saved Search icon (star icon) will appear, this time with a Replace option for the search you're updating. Click Replace to confirm.

The screenshot shows a 'Replace' dialog box. At the top, there are tabs for 'Save New' and 'Replace'. Below the tabs, the search name 'CCNs on Telegram' is displayed. At the bottom, there are 'Cancel' and 'Replace' buttons.

Your Trackers: Alerts Page

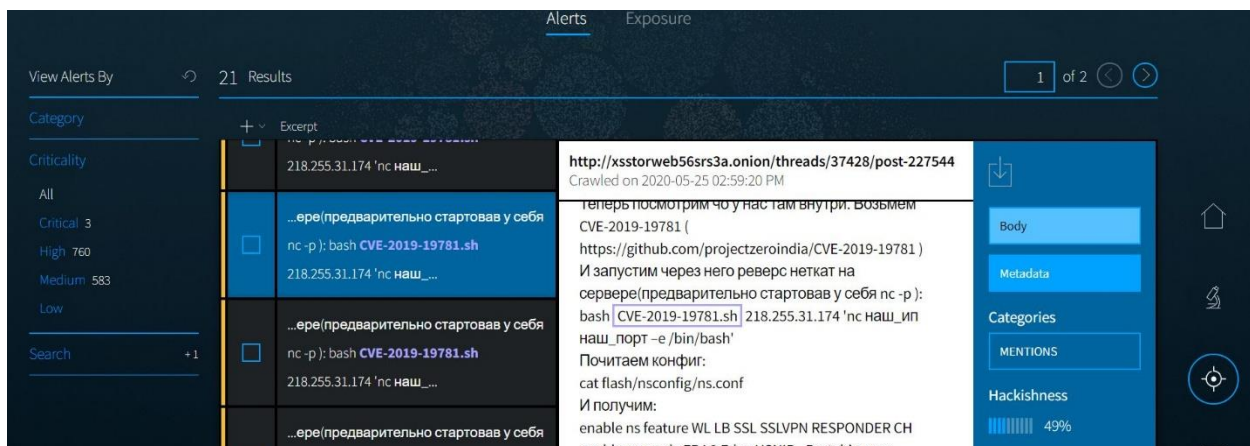
Access your **Alerts page** from the Trackers right navigation icon, or from the Alerts Dashboard.

Alerts are results found by your automated saved searches. Your Alerts dashboard (1) will display the number of active Critical, High, Medium, and Low results. If you have created categories, you can toggle the view to display by Criticality or Category (2). You can also get to your Alerts directly from the Trackers right navigation icon (3).



Alerts Page and Viewing Alerts

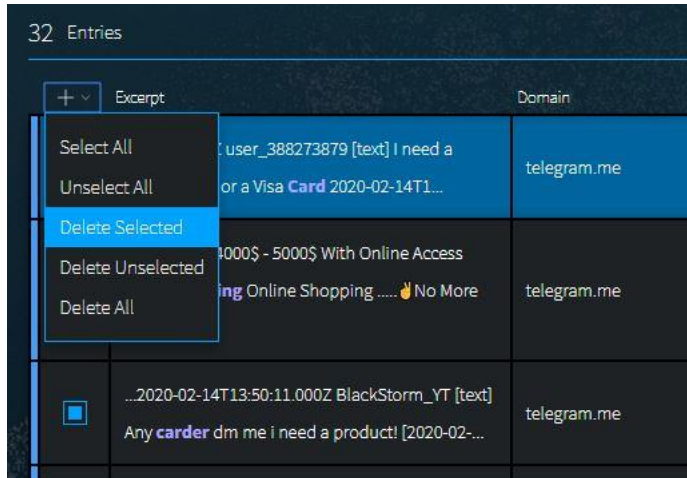
The Alerts page will display your result list. Each entry will include an excerpt from the result (around the first keyword match, if applicable), the location where the result was found, the Saved Search name, the Alert date, hackishness, and relevance of the result. Use the Filter By menu on the left to view Alerts ***by Category, by Criticality, or by Search Name.***



Deleting Alerts

Once alerts are reviewed and no longer needed, you can delete them from your result set. Select a set of results by checking the box(es), and then use the Action drop-down list. The drop-down list also gives a

bulk option to Delete All alerts. *Note: You may experience a browser delay when deleting multiple alerts, or alerts that are large in size.*



Your Trackers: DARKINT Exposure

DARKINT Exposure tracks your organization's DARKINT score over time, based on the *quantity*, *quality*, and *freshness* of exposed data on the dark web and interconnected data sources. Scores are generated with privacy-compliant data points, requiring only a website and email domain to calculate.

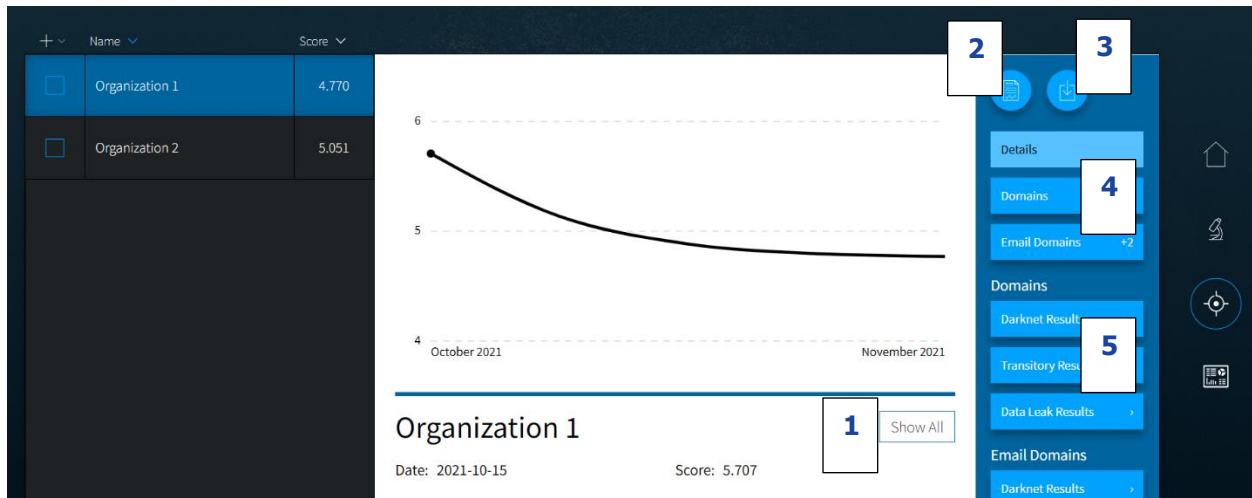
Access your **Trackers: DARKINT Exposure** page from the Trackers right navigation icon, or from the Dashboard. The Dashboard gives an at-a-glance view of all organizations you have set up. Click on an organization name to access more detail on the **Trackers: DARKINT Exposure** page.



On the **Trackers: DARKINT Exposure** page, hovering over the different points on the visualization will display the score inputs below the visualization.

1. Select the *Show All* button to compare the current organization with others that are set up.
2. Click the Report icon to generate a PDF an Exposure Score Report for the latest score.
3. Click the Download icon to download a CSV of all the scores and associated inputs that were generated for this organization.

- Click the Domain and Email Domain buttons to see the inputs used in the formula.
- Click the buttons below Domains or Email Domains to see the results that generated the score.



Setting Up a Score

Create a score by clicking on the + icon on the **Trackers: DARKINT Exposure** page.

The 'Add Score' form contains the following fields and options:

- Name:** A text input field with the placeholder 'Organization Name'.
- Domains:** A text input field with the placeholder 'organization.com'.
- Email Domains:** A text input field with the placeholder 'orgemail.com'.
- Email me when this score increases:** A checkbox that is currently checked.
- Buttons:** 'Cancel' and 'Submit' buttons at the bottom right.

- Type the Name that will be displayed in your score list.
- Add one or more domains and subdomains, if any.
- Add one or more email domains and subdomains. Only the domain portion is required; the @ symbol is not necessary.
- If desired, check the box to receive email notifications when your score increases.
- Click **Submit**.

At initial setup, scores will be generated for the previous month, and will continue to generate weekly.

+	Name	Score	Change	Trend	Last Run
<input type="checkbox"/>	Organization 1	4.770	▼ -0.026		2021-11-12
<input type="checkbox"/>	Organization 2	5.051	▲ 0.257		2021-11-12

The DARKINT Score Formula

$$\text{DARKINT SCORE} = H_{90}(\ln \text{RDS} + \ln \text{RTS}) + H_{\text{ATR}}(\ln \text{ATR})$$

H_{90} = Hackishness of last 90 days results

H_{ATR} = Hackishness of all time Data Leak results

RDS = # results from Darknet Sites

RTS = # results from Transitory Sites

ATR = # results from all time Data Leak results

Scores are logarithmic, meaning every point reflects almost triple the profile of a single point less.

The algorithm focuses on specific DARKINT sources for unique matches on an organization's website and email domains, and adjust the results based on hackishness. *Hackishness is the most critical input to the score*, as it eliminates uninteresting content hits. We find it critical to differentiate between overall hits and hackish hits; simply because a piece of information is found on the darknet does not necessarily make it problematic to an organization.

Recent results within the last 90 days are given the most weight, as recent breaches or data leaks containing an organization's proprietary information are often more useful to hackers, and potentially haven't yet been mitigated.

Viewing Scores Over Time

DARKINT Exposure Scores are the first metric to measure an organization based purely on dark web intelligence. Increasing scores may correlate to heightened risk profiles. Tracking scores over time, changes can indicate progress in hardening security, or alert to the presence of breaches or data leaks.

Scores are:	Scores are <i>not</i> :
<ul style="list-style-type: none"> A point-in-time snapshot An assessment of hackish data accessible 	<ul style="list-style-type: none"> A "risk of breach" Indicative of all risks facing a group